CHAPTER 1

Introduction

This document contains information about downloading and installing Cisco IOS Release 12.2(33)SCA. It also provides new and changed information, hardware support, limitations and restrictions, and caveats for Cisco IOS Release 12.2(33)SCA.

For software caveats that apply to the Cisco IOS Release 12.2(33)SCA on the Cisco uBR7200 series routers, see the corresponding release notes for Cisco uBR7200 Series Routers.

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/en/US/customer/support/tsd_products_field_notice_summary.html.

If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

This chapter includes the following sections:

Inheritance Information

This section describes the related Cisco IOS software releases that are part of the Cisco IOS Release 12.2SC train.

SCA-based releases

- Prior Cisco IOS 12.2SCA releases
- Cisco IOS Release 12.3(21)BC
- Cisco IOS Release 12.2(31)SB (which is based on Cisco IOS Release 12.2(25)S and includes many features from Cisco IOS Release 12.2T)
- Cisco IOS Release 12.2(33)SRC

System Requirements

These sections describe the system requirements for Cisco IOS Release 12.2(33)SCA:

- Memory Requirements, page 1-2
- Hardware Supported, page 1-2
- Verifying the Software Version, page 1-5
- Upgrading to a New Software Release, page 1-5
- Microcode Software, page 1-8
- Feature Support, page 1-8

Memory Requirements

This section describes the memory requirements for Cisco IOS Release 12.2(33)SCA.

Table 1-1 displays the memory recommendations for the Cisco uBR10012 universal broadband router with Cisco IOS Release 12.2(33)SCA feature sets.

Table 1-1 Memory Recommendations for the Cisco uBR10012 Router

Feature Set	Cisco uBR10012 Route Processor	Software Image	Recommended Flash Memory	Recommended DRAM Memory[1]	Runs From
DOCSIS Base 3 DES image and Lawful Intercept for Cisco PRE2[2]	PRE2	ubr10k2-k9p6u2-mz	128 MB	1.0 GB	RAM

[1] DRAM memory is not configurable on the Cisco uBR10012 router.

[2] PRE = Performance Routing Engine

Hardware Supported

The following sections list the hardware supported on various Cisco IOS Releases:

- Cable Interface Line Cards Supported, page 1-2
- Microcode Software, page 1-8
- Other Hardware Supported, page 1-5

Cable Interface Line Cards Supported

Table 1-2 provides information about the cable interface line cards supported in Cisco IOS Release 12.2(33)SCA.

Table 1-2 Cable Interface Line Cards Supported in Cisco IOS Release 12.2(33)SCA

Supported Cable Interface Line Card	Minimum Cisco IOS Release Required	Processor Engine
Cisco uBR10-MC5X20S/U/H—maximum 8	Cisco IOS Release 12.2SCA	PRE2

OIR of Cable Interface Line Cards on the Cisco uBR10012 Universal Broadband Router

The Cisco uBR10012 series universal broadband routers support online insertion and removal (OIR) of cable interface line cards only when exchanging cable interface line cards of the same type.

Prerequisites for Performing OIR

- Save the line card configuration before starting the OIR.
- Perform OIR when the CMTS is up and running.
- Change the standby card (if available) to HOT state.
- Save the startup configuration file before any reload of the system (if there is a need to reload), after a successful OIR.

Restrictions During OIR Process

- OIR upgrade cannot be performed when the standby PRE is being loaded.
- OIR downgrade from the Cisco UBR-MC20X20V line card to the Cisco uBR10-MC5X20 line card may fail in certain scenarios when the frequency and RF power settings on the Cisco UBR-MC20X20V line card are incompatible with the Cisco uBR10-MC5X20 card.

Performing an OIR of a Cable Interface Line Card

Step 1 In global configuration mode, enter the **cr10k card oir-compatibility** command for the cable interface line card to perform an OIR, as shown in the following example:

```
Router(config)# cr10k card 8/0 oir-compatibility
```

This command helps preserve the configuration and performs some internal synchronization to make sure that the OIR runs successfully.

Step 2 Save the configuration to ensure the transition, as shown in the following example:

```
Router# copy running-config startup-config
```

Step 3 Turn the power off to the line card using the **cable power off** command for the slot that is being replaced, as shown in the following example:

```
Router# cable power off 8/0
Line Card 8/0 is POWERED OFF
```

This powers off the line card gracefully.

Step 4 Before removing the card, verify that the proper grounding instructions have been followed for the card.

For more information about preventing electrostatic discharge (ESD) damage, see:

http://www.cisco.com/warp/public/109/cable-linecard-handling.pdf

Step 5 Remove the line card.

Step 6 Replace it with the new line card in the slot.

Step 7 Enter the **cable power on** command to power up the line card, as shown in the following example:

```
Router# cable power on 8/0
```

Step 8 Enter the **show interface cable** command and verify that the card and line protocol is “up” as shown in the following example:

```
Router# show interface cable 8/0/0

Cable8/0/0 is up, line protocol is up
```

```
  Hardware is BCM3210 ASIC, address is 000a.13e8.1ca8 (bia 000a.13e8.1a60)
  Internet address is 10.1.1.3/24
  MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation, loopback not set, keepalive not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 4d07h, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queuing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1834000 bits/sec, 2385 packets/sec
  5 minute output rate 1982000 bits/sec, 2431 packets/sec
      24461542 packets input, 2348214388 bytes, 0 no buffer
      Received 1979 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      24854257 packets output, 2536222931 bytes, 0 underruns
      0 output errors, 0 collisions, 0 interface resets
      0 output buffer failures, 0 output buffers swapped out
```

Step 9 Enter the **show controllers cable** command and verify the hardware status, as shown in the following example:

```
Router# show controllers cable 8/0/0
Cable8/0/0 JIB hardware status:
  JIB Downstream port   Enabled
  JIB Upstream   port 0 Enabled
  JIB Upstream   port 1 Enabled
  JIB Upstream   port 2 Enabled
  JIB Upstream   port 3 Enabled
Cable8/0/0 Upconverter is Enabled Output is Enabled
  Model: 74-3153-02 Serial Number: 0WAV090200A1 CLEI Code: FFFFFFFFFF
  HW Rev:    PC2D0109 SW Rev: 203, NVRAM Rev: 021 ECI numb
```

Note To verify the hardware status of the Cisco UBRMC20X20V cable line cards, it is recommended that you run the **show controller integrated-cable 8/0/0 brief** command instead of the **show controllers cable** command.

Step 10 Verify the configuration with the **show running-configuration** command.

Cisco uBR10012 Universal Broadband Router Line Cards Supported

The Cisco uBR10012 universal broadband router supports up to four network line cards with any combination of the following cards:

- Cisco Half-Height Gigabit Ethernet (HHGE) line card
- Cisco uBR10012 OC-48 DPT/POS interface module

Other Hardware Supported

Table 1-3 provides information about other hardware supported in Cisco IOS Release 12.2(33)SCA.

Table 1-3 Other Hardware Supported in this Cisco IOS Release

Hardware	Cisco uBR10012 Router	Minimum Cisco IOS Release
Cisco Wideband SIP and Cisco Wideband SPA	Yes	Cisco IOS Release 12.2(33)SCA
Cisco uBR10012 universal broadband router TCC+ card	Yes	Cisco IOS Release 12.2(33)SCA

Verifying the Software Version

To determine the version of the Cisco IOS software running on your Cisco universal broadband router, log in to the router and enter the **show version** EXEC command:

```
Router# show version

Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M), Version 12.2(33)SCA
EXPERIMENTAL IMAGE ENGINEERING C10K_WEEKLY BUILD, synced to
MAYFLOWER_BASE_FOR_V122_33_SA_THROTTLE
Copyright (c) 1986-2008 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 12.4(12.2r)T, RELEASE SOFTWARE (fc1)
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, see "How to Choose a Cisco IOS Software Release" at the following location:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml

For information about upgrading the Cisco universal broadband routers, see the *Software Installation and Upgrade Procedures* document at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094c07.shtml

For Cisco IOS upgrade ordering instructions, see:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at the following URL:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

Upgrading to Cisco IOS Release 12.2(33)SCA on a Cisco uBR10012 Universal Broadband Router

A cold start of the router is recommended for an upgrade to Cisco IOS Release 12.2(33)SCA on a Cisco uBR10012 universal broadband router from a different release train, such as Cisco IOS Release 12.3(23)BC or other BC releases.

If you are supporting PRE1 or earlier processors, it is also required to upgrade to PRE2 processors to support Cisco IOS Release 12.2(33)SCA.

Upgrading from ESR-PRE1 to ESR-PRE2 Processors

Upgrading a system that currently uses an ESR-PRE1 (or earlier processor) requires a hardware upgrade to an ESR-PRE2 to run Cisco IOS Release 12.2(33)SCA. For hardware installation instructions, see the *Cisco Performance Routing Engine (ESR-PRE2) Upgrade Installation* document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/cable/performance_routing_engine/quick/start/pre2_qsg.html

Upgrading from Cisco IOS Release 12.3BC or Earlier Cisco IOS Software Release

To upgrade from Cisco IOS Release12.3BC or earlier Cisco IOS software release, perform the following steps for an ESR-PRE2 cold start.

This procedure assumes the following configuration:

- Cisco uBR10012 chassis with two installed ESR-PRE2 processors
- A non-upgrade-enabled image such as Cisco IOS Release 12.3BC or earlier on the PRE2s

Note The router will not be available for user traffic during Step 7 of the software upgrade, and traffic cannot resume until the upgrade is complete.

To identify the key differences in the Cisco IOS Release SC train, see Important Notes, page 1-21

To perform the upgrade, follow these steps:

Step 1 Load the appropriate Cisco IOS Release 12.2SC image from the TFTP server into bootflash on both ESR-PRE2s.

Step 2 If the startup configuration is not up to date, save the running configuration using the **write-memory** command.

Step 3 Copy the startup configuration from the active ESR-PRE2 to a disk or TFTP server to save it for possible rollback.

Step 4 At the console, use the **boot system bootflash:***image_name* command to edit your boot system variable to point to the Cisco IOS Release12.2SC image in bootflash. Save the running configuration using the **write memory** command.

Use the **show bootvar** command to verify that the boot system variable has been altered appropriately on both the active and standby ESR-PRE2s.

If you do not want to make further changes to the startup configuration for the new command set offered by Cisco IOS Release 12.2SC, skip to Step 7.

Note In some older releases, the configuration does not explicitly specify the redundancy mode. If your current configuration is one of these, and you want RPR+ operation with Cisco IOS release 12.2SC, you must add the line **mode rpr-plus** after the line that specifies redundancy in the configuration on the TFTP server. Cisco IOS Release 12.2SC defaults to SSO mode unless it is explicitly configured for RPR+.

Step 5 Your startup configuration now reflects the altered boot system image. Copy it to the TFTP server and make any other needed edits. Then copy the altered configuration from the server to the startup configuration on the active and standby ESR-PRE2s using the **copy tftp startup** and **copy tftp stby-nvram:startup-config** commands. Verify that the startup configuration has been copied to both the active and the standby NVRAM using the **dir** command and comparing file size.

Step 6 Verify again that the boot image and config-register are set appropriately using the **show bootvar** command.

Step 7 On the active ESR-PRE2, enter the **reload** command and type **no** if you are asked to save the running configuration.

- If the system is configured for autoboot, it will autoboot the new 12.2SC image on both ESR-PRE2s.
- If the system is not configured for autoboot, both ESR-PRE2s will come up in ROM monitor after reloading. Boot the 12.2SC image in bootflash from the ROM monitor prompt on each ESR-PRE2.

At this point, the system should be operating as a dual-PRE redundant Cisco IOS Release 12.2(28)SB system in the configured mode (either SSO or RPR+), running the properly modified startup configuration. You can verify the redundancy status using the **show redundancy** or **show redundancy state** command.

Step 8 Enter the **write memory** command from the active console to bring the startup configuration up to date on the active and standby ESR-PRE2s.

Rollback Procedure

To roll back to the original release:

Step 1 Copy the original startup configuration from the TFTP server to the startup configuration on the active and standby ESR-PRE2s using the **copy tftp startup** and c**opy tftp stby-nvram:startup-config** commands. (This is the configuration file you copied in Step 3 of the upgrade procedure.)

Step 2 Use the **show bootvar** command to verify that the boot system variable now points to the old image and the config-register is set appropriately.

Step 3 Reload the active ESR-PRE2 using the **reload** command.

- If autoboot is set, the system should come up in the configured redundant mode (for older releases that support redundancy).
- If autoboot is not set, the system will come up to ROM monitor. From the ROM monitor prompt, boot the proper image from the bootflash on each ESR-PRE2.

You have now reverted to the original system configuration.

Microcode Software

This section describes microcode software that is supported for the Cisco uBR10012 router.

SPA FPD Image Packages for the Cisco uBR10012

The field-programmable device (FPD) image packages are used to update the shared port adapter (SPA) FPD images. If a discrepancy exists between a SPA FPD image and the Cisco IOS image that is running on the router, the SPA is deactivated until this discrepancy is resolved.

Note The maximum time to upgrade the FPD image on one SPA is 2 minutes. The total FPD upgrade time depends on the number of SPAs.

Note The FPD image package that is used to upgrade SPAs on a router that runs Cisco IOS Release 12.2(33)SCA is the ubr10k-fpd-pkg.122-33.SCA pkg file.

Table 4 Shared Port Adapter FPD Image Package Contents

Supported SPAs	FPD ID	FPD Component Name	FPD Component Version	Minimum Required Hardware Version
Cisco Wideband SPA	1	BLAZE FPGA	1285.1446	0.0

Upgrading from Cisco IOS Release 12.3BC or Earlier Cisco IOS Software Release

For more information, see the *Cisco uBR10012 Router Release Notes for Cisco IOS Release 12.2(33)SCA* at the following URL:

http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_release_notes_list.html

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser or user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Cisco CMTS User Documentation References for Cisco IOS Release 12.2SC

Table 1-5 provides information about the important user guides in Cisco IOS Release 12.2SC.

Table 1-5 Important Guides in Cisco IOS Release 12.2SC

Guide	Description
Documentation Roadmap	Describes a set of Cisco CMTS documents and contains links to the referenced documents. Go to the following link to access this document: http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr10012/roadmap/u10krdmp.html
Command Reference	Provides information about the software commands used to configure a Cisco CMTS. Includes command syntax, default value, value range, command mode, usage guidelines, and examples. Go to the following link to access this document: http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Design Guides	Describes how to plan, install, and configure a Cisco CMTS. Contains information about the supported technologies, interfaces and protocols and can also contain special installation considerations, network diagrams, example applications, system design, and environmental recommendations. Go to the following link to access this document set: http://www.cisco.com/c/en/us/support/video/ubr10000-series-universal-broadband-routers/products-implementation-design-guides-list.html
Install and Upgrade Guides	Provides step-by-step instructions for installing or upgrading a Cisco CMTS. Also includes line card installation guides, shipping documents, safety information, and quick-start guides for experienced users. Go to the following link to access this document set: http://www.cisco.com/c/en/us/support/video/ubr10000-series-universal-broadband-routers/products-installation-guides-list.html
Configuration Guides	Contains detailed, step-by-step instructions for configuring a Cisco CMTS, including software feature guides, configuration examples, network diagrams, and technical concepts. Go to the following link to access this document set: http://www.cisco.com/c/en/us/support/video/ubr10000-series-universal-broadband-routers/products-installation-and-configuration-guides-list.html
Error and System Messages	Lists error and system messages for a Cisco CMTS, including any recommended user action for each message. Go to the following link to access this document: http://www.cisco.com/c/en/us/support/video/ubr10000-series-universal-broadband-routers/products-system-message-guides-list.html
Troubleshooting Guides	Provides problem-solving techniques for a Cisco CMTS, including methods to identify problems based on symptoms and recommended actions for resolution. Go to the following link to access this document set: http://www.cisco.com/c/en/us/support/video/ubr10000-series-universal-broadband-routers/products-troubleshooting-guides-list.html

Cisco Feature Navigator

The Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side-by-side to display both the features unique to each software release and the features that the releases have in common.

To access the Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check verifies that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password is e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

https://tools.cisco.com/RPF/register/register.do

The Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

For frequently asked questions about the Cisco Feature Navigator, see the FAQs at the following URL:

http://www.cisco.com/support/FeatureNav/FNFAQ.html

Determining Which Software Images Support a Specific Feature

To identify the software images (feature sets) in Cisco IOS Release 12.2(33)SC that support a specific feature:

Step 1 Go to the Cisco Feature Navigator home page. Enter your Cisco.com login.

Step 2 Click **Search by Feature**.

Step 3 To find a feature, use either **Filter by full or partial feature name** or search for available features in alphabetical order. Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list is displayed in the text box.

Step 4 Select a feature from the Available Features pane, and click **Add** to add a feature to the Selected Features pane.

Note To learn more about a feature in the list, click **Show Descriptions**.

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

Step 5 Click **Continue** when you are finished selecting features.

Step 6 From the Major Release drop-down menu, choose **12.2SC**.

Step 7 From the Release drop-down menu, choose the appropriate maintenance release.

Step 8 From the Platform Family drop-down menu, select the appropriate hardware platform. The **Search Results** table lists all the software images (feature sets) that support the selected feature.

Determining Which Features Are Supported in a Specific Software Image

To determine the features supported in a specific software image (feature set) in Cisco IOS Release 12.2(33)SC:

Step 1 Go to the Cisco Feature Navigator home page. Enter your Cisco.com login.

Step 2 Click **Compare Images**.

Step 3 From the Software drop-down menu in the **Select First Image Parameters** pane, choose **IOS**.

Step 4 From the Major Release drop-down menu, choose **12.2SC**.

Step 5 From the Release Number drop-down menu, choose the appropriate maintenance release.

Step 6 From the Platform Family drop-down menu, choose the appropriate hardware platform.

Step 7 From the Feature Set drop-down menu, choose the appropriate feature set. The **Search Results** table lists all the features that are supported by the selected feature set (software image).

New and Changed Information

The following sections list the new and modified hardware and software features supported on the Cisco uBR10012 universal broadband routers in Cisco IOS Release 12.2(33)SCA and its maintenance-based releases:

- New Hardware Features in Cisco IOS Release 12.2(33)SCA2, page 1-11
- New Hardware Features in Cisco IOS Release 12.2(33)SCA1, page 1-11
- New Hardware Features in Cisco IOS Release 12.2(33)SCA, page 1-11
- New Software Features in Cisco IOS Release 12.2(33)SCA2, page 1-13
- Modified Software Features in Cisco IOS Release 12.2(33)SCA2, page 1-13
- New Software Features in Cisco IOS Release 12.2(33)SCA1, page 1-13
- Modified Software Features in Cisco IOS Release 12.2(33)SCA1, page 1-13
- New Software Features in Cisco IOS Release 12.2(33)SCA, page 1-13

New Hardware Features in Cisco IOS Release 12.2(33)SCA2

There are no new hardware features in Cisco IOS Release 12.2(33)SCA2.

New Hardware Features in Cisco IOS Release 12.2(33)SCA1

There are no new hardware features in Cisco IOS Release 12.2(33)SCA1.

New Hardware Features in Cisco IOS Release 12.2(33)SCA

This section describes the hardware features supported in Cisco IOS 12.2(33)SCA. Some features may be new to Cisco IOS Release 12.2(33)SCA but were released in earlier Cisco IOS software releases.

Cisco uBR10012 Support in Cisco IOS Release 12.2(33)SCA

This feature adds support for the Cisco uBR10012 universal broadband router in Cisco IOS Release 12.2(33)SCA. The Cisco uBR10012 router is previously supported in Cisco IOS Release 12.3BC.

The Cisco uBR10012 router provides a cost-effective, scalable, and industry-proven CMTS, optimized for aggregating traffic at the edge of the cable network. It has eight broadband aggregation slots and four WAN backhaul slots.

Designed for cable operators and service providers, the Cisco uBR10012 router CMTS platform connects residential subscribers via cable modems, digital set-top boxes, or IP telephony cable modems for high-speed data, broadband entertainment, and IP telephony solutions.

The Cisco uBR10012 router chassis is designed for front and rear access. The front of the chassis provides access to the following components:

- Two performance routing engine processor modules
- LCD display
- Two DC Power Entry Modules (DC PEMs)
- Fan assembly module

The rear of the chassis provides access to the following components:

- Eight cable interface line cards (single-slot)
- Four high-speed, high-performance network uplink interface line cards
- Two Timing, Communication, and Control Plus (TCC+) cards

The Cisco uBR10012 router uses redundant PEMs using –48 to –60 VDC input power. An optional AC-input power shelf can be used to provide the DC-output power for the Cisco uBR10012 router.

For more information on the Cisco uBR10012 router chassis and supported components, see the “Obtaining Documentation and Submitting a Service Request” section on page 1-22.

Cisco Wideband SIP and Cisco Wideband SPA

The Cisco uBR10012 router currently supports only the Cisco Wideband SIP for the 1-Gbps Wideband SPA (part number UBR10-2XDS-SIP). The Wideband SIP can support up to two Cisco 1-Gbps Wideband SPAs.

The Cisco Wideband SPA is a single-wide, half-height shared port adapter that provides Cisco Wideband Protocol for a DOCSIS Network formatting to the downstream data packets. The Wideband SPA is used for downstream data traffic only.

The Wideband SPA has one active and one redundant Gigabit Ethernet port that is used to send traffic to the external edge QAM device. If the link state of both Gigabit Ethernet ports is up, port 0 will come up as the active port and port 1 will be the redundant port. If the link state of port 0 is not up, port 1 will come up as the active port.

The Cisco uBR10012 router can support up to two Cisco Wideband SPAs. Depending on how it is configured, each Cisco Wideband SPA supports up to 24 RF channels. Each Cisco Wideband SPA can support up to 12 logical wideband channels (bonding groups).

The Wideband SPA contains field-programmable devices: the Wideband SPA FPGAs and Complex Programmable Logic Device (CPLDs). The FPGA and CPLD upgrade information is part of the Cisco IOS release rather than a separate file to be downloaded by users.

For more information about the Cisco Wideband SIP and Cisco Wideband SPA hardware and software, refer to the following documents for Cisco IOS 12.3(21)BC-based software releases:

- *Cisco uBR10012 Universal Broadband Router SIP and SPA Hardware Installation Guide*
- *Cisco uBR10012 Universal Broadband Router SIP and SPA Software Configuration Guide*

New Software Features in Cisco IOS Release 12.2(33)SCA2

There are no new software features in Cisco IOS Release 12.2(33)SCA2.

Modified Software Features in Cisco IOS Release 12.2(33)SCA2

There are no modified software features in Cisco IOS Release 12.2(33)SCA2.

New Software Features in Cisco IOS Release 12.2(33)SCA1

There are no new software features in Cisco IOS Release 12.2(33)SCA1.

Modified Software Features in Cisco IOS Release 12.2(33)SCA1

There are no modified software features in Cisco IOS Release 12.2(33)SCA1.

New Software Features in Cisco IOS Release 12.2(33)SCA

This section describes the new cable software features in Cisco IOS Release 12.2(33)SCA. Some features may be new to Cisco IOS Release 12.2(33)SCA but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.2(33)SCA. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included below. If a feature listed below does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided below.

DHCPv6 Relay Agent Notification for Prefix Delegation

DHCPv6 relay agent notification for prefix delegation allows the router working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 RELAY-REPLY packet that is being relayed by the relay agent to the client. When a prefix delegation option is found by the relay agent, the relay agent extracts the information about the prefix being delegated and inserts an IPv6 static route matching the prefix delegation information onto the relay agent. Future packets destined to that prefix via relay will be forwarded based on the information contained in the prefix delegation. The IPv6 static route is then left in the routing table until the prefix delegation lease time expires or the relay agent receives a release packet from the client releasing the prefix delegation.

No user configuration is required for this feature. Static route management is done automatically by the relay agent.

The IPv6 routes are added when the relay agent relays a RELAY-REPLY packet, and the IPv6 routes are deleted when the prefix delegation lease time expires or the relay agent receives a release message. An IPv6 static route in the routing table of the relay agent can be updated when the prefix delegation lease time is extended.

This feature leaves a static IPv6 route on the routing table of the relay agent. This registered IPv6 address allows unicast reverse packet forwarding (uRPF) to work by allowing the router doing the reverse lookup to confirm that the IPv6 address on the relay agent is not malformed or spoofed. The static route left in the routing table of the relay agent can be redistributed to other routing protocols to advertise the subnets to other nodes. The static routes will be removed when an DHCP_DECLINE message is sent by the client.

For detailed information about this feature, see the "Implementing DHCP for IPv6" chapter of the *Cisco IOS IPv6 Configuration Guide* at:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html

IPv6 on Cable

In Cisco IOS Release 12.2(33)SCA, IPv6 functionality is introduced on the Cisco universal broadband routers. IPv6 (Internet Protocol Version 6) has also been called "IPng" (IP Next Generation). Formally, IPv6 is a set of specifications from the Internet Engineering Task Force (IETF) that were designed as an evolutionary set of improvements to the current IP Version 4. The most obvious difference between IPv6 and IPv4 is that IP addresses are lengthened from 32 bits to 128 bits, which dramatically increases the available number of IP addresses as expanding network technologies and the need for IP addressing on multiple consumer devices is straining the current IPv4 address space.

There are many areas of IPv6 support available in Cisco IOS Release 12.2(33)SCA that are platform-independent and therefore, are also supported by the Cisco CMTS routers. In addition to these platform-independent features in the Cisco IOS software, there are DOCSIS 3.0 IPv6 features and legacy cable features that are modified for support of IPv6.

The IPv6 on Cable feature documentation provides references to the currently documented platform-independent features in the Cisco IOS software documentation, as well as a list of the unsupported platform-independent features. Support for new DOCSIS 3.0 IPv6 features and modifications to legacy cable features are included in this documentation.

For detailed information about this feature, see the Cisco feature document at:

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_ipv6.html

L2VPN Support over Cable

In Cisco IOS Release 12.2(33)SCA, the Layer 2 VPN (L2VPN) Support over Cable feature on the Cisco CMTS provides point-to-point Transparent LAN Service (TLS) in support of the Business Services over DOCSIS (BSOD) CableLabs specification.

The L2VPN Support over Cable feature in Cisco IOS release 12.2(33)SCA differs from prior L2VPN and TLS support for cable in Cisco IOS release 12.3BC in the following ways:

- Both features use an Ethernet trunking interface to transport traffic for multiple L2VPN tunnels in support of different cable modems (CMs) and service flows (SFs) based on IEEE 802.1q VLAN IDs. For the legacy TLS service, only the primary upstream or downstream SFs are used. With the new L2VPN Support over Cable feature, both primary and secondary SFs can be used.
- The TLS feature uses CLI to provision the service. The L2VPN Support over Cable feature uses the CM configuration file to provision the service, and a single CLI to identify the default Ethernet Network System Interface (NSI) interface.

- Downstream traffic is forwarded on a per-CM basis and upstream traffic is forwarded on a per-SF basis. For L2VPN Support over Cable, upstream traffic for the same L2VPN can use multiple upstream service flows and downstream traffic can use different downstream service flows.

For detailed information about this feature, see the Cisco feature document at:

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_l2vpn.html

MPLS HA

The Multiprotocol Label System (MPLS) high availability (HA) features provide SSO and NSF capability to the MPLS Label Distribution Protocol (LDP) and MPLS Virtual Private Network (VPN) features.

The following MPLS HA features have the ability to continue forwarding data following a PRE2 switchover on the Cisco uBR10012 universal broadband router:

- MPLS Label Distribution Protocol (LDP)
- MPLS Virtual Private Networks (VPNs)

When you enable MPLS HA, you get the benefit of allowing a PRE2 on the Cisco uBR10012 universal broadband router to recover from disruption in service without losing its LDP bindings, MPLS forwarding state, and VPN prefix information.

Restrictions for MPLS HA

- Any Transport over MPLS (AToM) is not supported.
- IPv6 over MPLS is not supported.
- Supports MPLS/HA with the following restrictions for Cisco Express Forwarding (CEF) scalability:
  - Up to 1 million prefixes
  - Up to 1 million adjacencies
  - Up to 1000 Virtual Routing and Forwarding instances (VRFs)
  - Arbitrary prefix path counts from the RIB
  - 8 paths per prefix for forwarding

For an overview of MPLS HA and more information about these features, refer to the “MPLS High Availability: Overview” document at:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fshaov.html

Multicast VPN and DOCSIS 3.0 Multicast QoS support

In Cisco IOS Release 12.2(33)SCA, the Cisco universal broadband routers support the following multicast features:

- Encrypted multicast within MVPNs
- DOCSIS 3.0 multicast QoS and admission control
- IGMP-only multicast echo

The Multicast VPN (MVPN) feature allows a service provider to configure and support multicast traffic in a MPLS-VPN environment. This feature supports routing and forwarding of multicast packets for each individual VPN routing and forwarding (VRF) instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

The MVPN feature allows an Internet service provider (ISP) to provide its MPLS-VPN customers the ability to transport their Multicast traffic across MPLS packet-based core network. The C-Multicast packet is encapsulated inside a P-Packet with a configured multicast address, instead of the usual MPLS tagging. Supported encapsulation methods include a GRE tunnel and IP-IP.

As part of the multicast enhancements introduced in Cisco IOS Release 12.2(33)SCA, the Cisco universal broadband routers also support DOCSIS 3.0 Multicast QoS. The implementation consists of group QoS configuration (GQC) in global configuration and association of a particular GQC with a physical downstream interface in interface configuration mode. The Multicast QOS profile defines the necessary information for GQC, and the association with a physical interface provides the MAC Domain and downstream channel set (DCS) information.

In the enhanced multicast echo feature, the Layer 3 multicast switching path uses a parallel express forwarding (PXF) multicast routing table instead of the existing multicast echo path. Therefore, upstream packets are echoed using the Layer 3 switching path and all upstream data packets are treated similarly to the ingress packets from a WAN interface, in which they pass through existing classifiers and service flows.

Intelligent multicast admission control explicitly acknowledgments of the establishment of each multicast session, does not consume additional bandwidth for multicast flows once the first flow is established, and cleans up service flows as the multicast session is torn down.

Restrictions for Multicast VPN and DOCSIS 3.0 Multicast QoS

- IPv6 is not supported.

For detailed information about this feature, see the Cisco feature document at:

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/CMTS_enhanced_multicast_ps2209_TSD_Products_Configuration_Guide_Chapter.html

NSF/SSO

Cisco Nonstop Forwarding (NSF) and Stateful Switchover (SSO) allows for continuous packet forwarding during a route processor (RP) fail over. This feature adds NSF/SSO support in Cisco IOS Release 12.2(33)SCA for the Cisco uBR10012 router, specifically for the DOCSIS protocol.

To protect the system from an RP failure, two RPs are used. One RP is the Active RP and the other is the Standby RP. If the Active RP becomes inactive because of hardware or software failure, the router can switchover to the Standby RP. SSO maintains the Layer 2 connectivity protocols between devices while NSF continues to forward IP packets during the route convergence time. The result is a transparent RP failure; there are no loss sessions or route flaps in the network.

In Cisco IOS Release 12.2(33)SCA, SSO is the default Performance Routing Engine (PRE) redundancy behavior on the Cisco uBR10012 Universal Broadband Router, with Route Processor Redundancy (RPR) as the fallback mode. In this release you can change the redundancy mode using the **mode** redundancy configuration command.

You can force a PRE switchover using the **redundancy force-switchover main-cpu** privileged EXEC command from either the primary or standby PRE. If you force a switchover from the active PRE, the PREs synchronize and the active PRE reloads normally. When you force a switchover from the standby PRE, a crash dump of the active PRE occurs by design for troubleshooting purposes. Forcing a switchover from the standby PRE should only be done if you cannot access the active PRE.

The following new commands or keywords are introduced in this release:

- **debug ehsa**
- **debug redundancy idb-sync-history**

- **redundancy force-switchover main-cpu**
- **show redundancy config-sync failures**
- **show redundancy idb-sync-history**
- **show redundancy platform**

For more information about redundancy features and High Availability on the Cisco CMTS routers, see the *Cisco IOS CMTS Cable Software Configuration Guide* at:

http://www.cisco.com/web/techdoc/cable/Config/Sw_conf.html

The following sections provide more information about other NSF/SSO-related features:

MPLS HA

The Multiprotocol Label System (MPLS) high availability (HA) features provide SSO and NSF capability to the MPLS Label Distribution Protocol (LDP) and MPLS Virtual Private Network (VPN) features.

The following MPLS HA features have the ability to continue forwarding data following a PRE2 switchover on the Cisco uBR10012 universal broadband router:

- MPLS Label Distribution Protocol (LDP)
- MPLS Virtual Private Networks (VPNs)

When you enable MPLS HA, you get the benefit of allowing a PRE2 on the Cisco uBR10012 universal broadband router to recover from disruption in service without losing its LDP bindings, MPLS forwarding state, and VPN prefix information.

Restrictions for MPLS HA

- Any Transport over MPLS (AToM) is not supported.
- IPv6 over MPLS is not supported.
- Supports MPLS/HA with the following restrictions for Cisco Express Forwarding (CEF) scalability:
  - Up to 1 million prefixes
  - Up to 1 million adjacencies
  - Up to 1000 Virtual Routing and Forwarding instances (VRFs)
  - Arbitrary prefix path counts from the RIB
  - 8 paths per prefix for forwarding

For an overview of MPLS HA and more information about these features, refer to the “MPLS High Availability: Overview” document at:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fshaov.html

OSPF Graceful Restart

This feature adds support for OSPF Graceful Restart feature in support of RFC 3623 in Cisco IOS Release 12.2SC. OSPF Graceful Restart support is introduced in Cisco IOS Release 12.3(21)BC.

For more information about the OSPF Graceful Restart feature, refer to the “NSF—OSPF (RFC 3623 OSPF Graceful Restart” document at:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gr_ospf.html

Service Independent Intercept on the Cisco CMTS

In Cisco IOS Release 12.2SC, the Service Independent Intercept (SII) feature enhances the current Lawful Intercept (LI) capability for Cisco uBR10012 Universal Broadband Routers using SNMPv3.

In other Cisco IOS Releases prior to 12.2SC on the Cable Modem Termination System (CMTS) routers, LI capability includes the following support:

- Intercepts for voice traffic in PacketCable environments
- IP intercepts for SII using SNMPv3
- Command-line interface (CLI) for MAC intercepts

SII extends this LI capability in Cisco IOS Release 12.2SC by adding support for CPE-based and CM-based MAC intercepts using SNMPv3.

For detailed information about this feature, see the Cisco feature document at:

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_siiv2.html

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check verifies that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password is e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

For information about the MIBs supported by the Cisco universal broadband routers, see the *Cisco CMTS Universal Broadband Series Router MIB Specifications Guide*.

New and Changed MIB Information in Cisco IOS Release 12.2(33)SCA

The Cisco universal broadband routers include or add support for the following MIBs in Cisco IOS Release 12.2(33)SCA:

- CISCO-DOCS-EXT-MIB—Supports object cdxCmtsCmQosProfile to cdxCmtsCmTable to associate a cable modem with a qos profile
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB—Supports alarm filtering
- CISCO-IP-FORWARD-MIB
- CISCO-IP-MIB
- CISCO-802-TAP-MIB

- CISCO-TAP2-MIB
- CISCO-IP-TAP-MIB
- CISCO-PROCESS-MIB
- DOCS-CABLE-DEVICE-MIB
- DOCS-IF-MIB—Supports draft-ietf-ipcdn-docs-rfmibv2-05.txt
- DOCSIS-L2VPN-MIB
- DOCS-SUBMGT-MIB
- IF-MIB—Supports subinterfaces in the ifTable
- TCP-MIB
- UDP-MIB

Limitations and Restrictions

This section describes restrictions for the Cisco universal broadband routers in Cisco IOS Release 12.2(33)SCF.

Unsupported Hardware

For a list of unsupported hardware, see the End-of-Life and End-of-Sale Notices at:

http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_eol_notices_list.html

Software Feature Restrictions

This section describes other important guidelines or restrictions to consider when running Cisco IOS Release 12.2SC that might not yet be documented in the supporting customer documentation.

DOCSIS

- You cannot configure a US connector to more than one fiber node.

DTI Card Configuration

The Cisco uBR10012 universal broadband router TCC card does not work as expected when the startup configuration contains the configuration for a Cisco uBR10012 universal broadband router TCC+ card. To fix this issue, use the **no card** *slot***/***subslot* **2cable-tccplus** command and then configure the DTI card.

MIBs Restrictions

- IP-MIB is implemented as read-only. Writing is not supported for ipv6IPForwarding or ipv6IpDefaultHopLimit.
- docsIf3MdCfgMcastDsidFwdEnabled object is implemented as read-only.
- cdxBWQueueMaxDepth object sometimes reports a value out of range. The supported range is from 0 to 64, but the object sometimes returns a value of 128 when queried.

PacketCable

Payload Header Suppression (PHS) is not supported on wideband Embedded Media Terminal Adapters (eMTAs) for dynamic downstream service flows.

PCMCIA

While performing an OIR of the PCMCIA disk on PRE2, the System Event Archive (SEA) application and other applications such as IPDR write details to the PCMCIA disk on PRE2.

Before performing the OIR, the multiple system operator (MSO) must disable the write access to the PCMCIA disk on PRE2 using the **cable filesystem [enable|disable]** command. For more information, see the CSCsz77977.

PXF

Statistics for two different divert-rate limit (DRL) WAN-IP streams can momentarily overlap or collide and produce statistics that are lower than expected.

Redundancy

- Longer dropout times (about 6 seconds) can occur when you use the OIR method to trigger a cable line card switchover on the Cisco uBR10012 router. To repair or maintain a cable line card and get better switchover performance, use the **redundancy linecard-group switchover** command to trigger the line card switchover instead.
- Although the software does not prevent it, preconfiguring commands on a protect line card is not supported.
- A dynamic service-flow for a PacketCable call is not deleted during a line card switchover.
- Although the Cisco CMTS router is initially configured only for global N+1 redundancy, the **show running-configuration** command displays both global and legacy interface-level Hot-Standby Connection-to-Connection Protocol (HCCP) configuration when you change the redundancy mode configuration from SSO to RPR mode. If you switch back to SSO mode, both redundancy configurations are still shown.
- In very rare circumstances, after an N+1 switchover, upstream traffic that is using Baseline Privacy Interface (BPI) encryption is not received properly by the CMTS router. Input errors are logged on the interface and the **debug cable error** command shows error messages similar to the following:

  ```
  Cable5/1/4: Bad rx packet. JIB status code 0xA
  ```

The issue occurs on upstream channels that use a shared connector, where the other upstream channel using the same shared connector is on another downstream and is shutdown. To workaround this issue, you can activate the downstream and other upstream channel using the same shared connector or temporarily unshare the upstream connector.

Wideband

If you configure a wideband interface with more than one MAC domain host sharing the committed information rate (CIR) bandwidth, then the total wideband interface CIR bandwidth gets fragmented among the MAC domain (MD) hosts sharing the wideband interface CIR bandwidth.

The WB interface CIR bandwidth can be shared by multiple MAC domain hosts, and these MAC domain hosts could potentially be on the same or different cable line cards. As admission control for WB interfaces occurs on cable line cards, the available CIR bandwidth gets partitioned and is given to the MD hosts causing the bandwidth fragmentation. However if a typical service flow CIR is very small compared to the total CIR of the wideband interface, then this fragmentation is not visible until the CIR usage reaches very high levels close to the total interface bandwidth.

With certain bandwidth percentage configuration and traffic distribution, the overall link utilization of dynamic bandwidth sharing (DBS) can be as low as 85 percent. For example, this can occur if the traffic rate on a wideband interface is smaller than its configured bandwidth percentage, but the traffic rate on a modular-cable interface is much larger than its bandwidth percentage. The packet drops occur only on the modular-cable interface which has a larger amount of traffic than its bandwidth-percentage. To workaround this scenario, configure a higher bandwidth percentage to the modular-cable interface, which is larger than or equal to its expected or average traffic rate.

Important Notes

Note This section describes important changes in various Cisco IOS Releases that differ from support found in earlier software releases supported by the Cisco CMTS routers. This section is subject to change and is not intended to cover all changes found in the software. There may be other changes within the software that are not identified here, such as within the new and modified features. Closely read these release notes in their entirety, as well as review the related caveats documents for more information.

Table 6 identifies some of the key changes that you should consider when running Cisco IOS Release 12.2(33)SCA.

Table 6 Important Changes in Cisco IOS Release 12.2SC

Change Description	Release Introduced
Clearing Address Resolution Protocol (ARP) Entries Using the **clear arp** command can take about 15 seconds to remove all ARP table entries.	12.2(33)SCA
Reverse Path Forwarding RPF on the Cisco uBR10012 router requires configuration of the **ip verify unicast source reachable-via rx allow-default** command to properly interpret default routes.	12.2(33)SCA

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.